Commander, U.S. Fleet Forces Command

Navy Base, Station and Installation
Physical Security Assessment Report
Part 2

31 October 2013

Table of Contents

1. Overview

a. In response to the September 16, 2013 tragedy at the Washington Navy Yard, and as directed in the Chief of Naval Operations/Commandant of the Marine Corps joint letter “Base, Station, and Installation Physical Security Assessment” of September 23, 2013, Commander, U.S. Fleet Forces and Commander, Marine Forces Command conducted an Installation Security Quick Look assessment of current physical security and access control measures at U.S. Navy and Marine Corps owned and operated installations--these findings were reported on September 27, 2013. The “quick look” assessment focused on the adequacy of Navy and Marine Corps physical security directives, as well as compliance with all directives and policies governing physical security and access control.

b. Per the Secretary of the Navy’s memorandum, “Base, Station, and Installation Physical Security Assessment” of October 11, 2013, Commander, U.S. Fleet Forces and Commander, Marine Forces Command conducted a more thorough review of physical security on Naval Installations. This second physical security review expanded on the joint Navy and Marine Corps “quick look” assessment and determined whether current procedures are appropriate and adequate, and recommends what enhancements, improvements and innovations should be taken in the future. Both the previous "quick look" assessment and this more in-depth review are separate from all other investigations related to the fatal shooting at the Washington Navy Yard.

The specified tasks from the Secretary of the Navy’s Memorandum are:

(1) Identify any gaps in doctrine, organization, training, material, leadership and education, personnel, and facilities that affect security program execution.
(2) Validate procedures by which Commanding Officers determine the degree of contractor access to government installations and facilities.
(3) Examine procedures used in the Continuous Evaluation Program and uniform standards of compliance.
(4) Review Service access control policy and procedures and risk mitigation measures.
(5) Review Installation Command and tenant Command/Activity security procedures and supported/supporting relationships.
(6) Review requirements, resources, and priorities for security encompassing infrastructure enhancement, access control, law enforcement, military police, and information/personnel security manpower.

(7) Identify technology enhancement options to mitigate risk and offset resource shortfalls.

(8) Evaluate training and education programs to identify contributing factors and behavioral indicators of potentially violent actors and to increase commander awareness of the need for continuous evaluation.

(9) Review personal weapons policies and procedures for uniformity and enforcement.

(10) Assess the adequacy of current physical security doctrine to mitigate postulated threats.

(11) Identify barriers to physical security and access control policy implementation.

(12) Recommend enhancements, improvements, and innovations, if any, in procedures or policies that could improve our ability to provide security at our installations.

(13) Assess current procedures to control, possess, and stow personal firearms on installations in accordance with applicable law, while considering practical implications of effective implementation.

(14) Review the vetting and credentialing procedures within the Department of the Navy for base access and eligibility for security clearances while considering vetting and credentialing in the context of the broader Department of Defense procedures.

(15) Coordinate with the Assistant Secretary of the Navy (Manpower & Reserve Affairs) and the General Counsel of the Navy, as necessary, regarding the security clearance rapid reviews.

c. Navy Fleet Commanders assess a command's compliance with established guidance and directives primarily through periodic higher headquarters assessments and exercises. Prior to January 2013, Navy force protection assessment processes focused exclusively on antiterrorism program administration and did not evaluate an installation's ability to operationally execute that program at the tactical level. U.S. Fleet Forces recognized this shortfall, and established the Higher Headquarters Antiterrorism Operational Assessment, which is specifically designed to close this gap by focusing primarily on operational execution versus administrative compliance. This issue is addressed in detail in paragraph 2.f.; Finding 1.2; and Recommendations 1.2.1. and 1.2.2.

In the "quick look" assessment, U.S. Fleet Forces reported that the Navy was "in compliance with physical security protection standards." That assessment was based on a review of available data from antiterrorism program assessments and exercises completed over the past three years, which indicated installations have in place appropriate policies and procedures to execute their antiterrorism program satisfactorily and to establish an appropriate force protection posture.

During the course of this more extensive review, it became apparent that operational execution of program requirements varies and that not all installations are meeting fully the requirements of their antiterrorism plans and other installation policy directives. In short, the navy's force protection program needs to more effectively connect assessment, readiness reporting and risk analysis to resourcing. We need to establish a single, independent force protection resource sponsor, with the authority and responsibility to manage and fund all aspects of the navy's force protection program. And we need to better man, train, organize and equip security force personnel.

d. To develop this report, U.S. Fleet Forces leveraged the findings of a variety different sources, including the Navy Inspector General's Special Study on Antiterrorism and Force Protection, March 13, 2013; the U.S. Fleet Forces Force Protection Baseline Review 2013; the U.S. Fleet Forces Navy Antiterrorism Program Review 2010; and the Department of Defense Inspector General report on the Navy Commercial Access System. Additionally, U.S. Fleet Forces conducted a Navy-wide survey of Navy Regions, installations and Fleet Commanders for input regarding specific issues including:

   (1) Resourcing concerns related to installation security requirements.
   (2) Adequacy and appropriateness of security policies and requirements.
   (3) Training regarding violent behavior indicators and reporting.
   (4) Installation vetting and credentialing issues.
   (5) Recommended installation security enhancements, improvements, or innovations.

Finally, subject matter experts from the Deputy Under-Secretary of the Navy for Plans, Policy, Operations, and Integration; Commander, Navy Installations Command; the Naval Criminal Investigative Service; and the Navy Staff provided input regarding the report's findings and recommendations.

e. The logical next step, following review and promulgation of this report, will be to assign an Office of Primary Responsibility to address each recommendation.

2. Navy Approach to Force Protection

a. Assumptions (*Basis--drawn from a compilation of Presidential, Department of Defense, Department of the Navy and Combatant Commander guidance and directives detailed in Section 5 of this report.)*

(1) Everything cannot be protected against every threat. *Navy risk-tiered security strategy*

(2) Established Department of Defense vetting and credentialing processes ensure that those who have been properly vetted and credentialed are loyal, trustworthy and reliable--thereby mitigating the potential for insider attack. *Navy policy*

(3) Random Anti-terrorism Measures are an effective deterrence and interrupt terrorist operational planning. *Navy policy*

(4) The conduct of 100 percent vehicle, personnel and baggage checks in Force Protection Condition Alpha is not required (lack of reporting indicating a specific, credible threat). *Navy policy*

(5) Department of Defense credentialing programs enable use of a trusted traveler policy in Force Protection Condition Alpha as authorized by the Secretary of Defense Directive Type Memorandum 09-12. *Department of Defense policy*

(6) The intelligence community's threat analyses are accurate. *Navy policy*

(7) Based upon the intelligence community's assessment, the threat to Navy forces in the Continental United States is low. *U.S. Fleet Forces assessment analysis*

(8) Existing installation Mutual Support Agreements with off-base agencies are executable. *Navy policy*

(9) Current Navy Force Protection training is sufficient and focused on the correct threats. *Navy policy*

(10) Installation and external agency response forces will rapidly mitigate and neutralize a potential threat. *Navy policy*

b. **Force Protection Policies and Guidance.** The Geographic Combatant Commander exercises Tactical Control for Force Protection of all Department of Defense forces in the commander's Area of Responsibility. The delegation of Tactical Control for Force Protection by the Geographic Combatant Commander is most commonly implemented along Service or functional component lines or geographically determined sectors. Once designated by the Geographic Combatant Commander, Navy Fleet Commanders further define the Tactical Control for Force Protection chain of command for Navy forces, to include Navy installations and tenants located within each Area of Responsibility. Each Fleet Commander promulgates this Tactical Control for Force Protection chain of command by Operations Order or instruction.

Geographic Combatant Commanders and the Services provide broad physical security policy which commanders use, combined with the results of risk assessments, to promulgate physical security guidance and directives to set an appropriate force protection posture. Commanders ensure continued compliance with and execution of all physical security guidance and directives through higher headquarters assessments and periodic observation of exercises.

Navy force protection is aligned with higher headquarters directives and is intended to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities and critical information. Physical security, as a sub-set of force protection, is concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material and documents; and to safeguard them against espionage, sabotage, damage and theft.

c. **Force Protection Implementation and Execution.** The Navy implements physical security through a defense-in-depth model based on the Department of Defense Antiterrorism Standard 13 (detect, assess, communicate, delay, deny and respond).

By design, the Navy's defense-in-depth model is intended to protect assets and personnel from external threats through the prevention of unauthorized access to our installations, either through denial of access or, if necessary, the use of lethal force. Inherent in the Navy's physical security model is the assumption that established vetting and credentialing processes ensure that those who have been properly vetted and credentialed are loyal, trustworthy and reliable--thereby mitigating the potential for insider attack. Additionally, Navy's physical security model includes the use of Random Antiterrorism Measures and a rapid, robust response capability to discourage the would-be insider.

The Navy uses a risk-based security strategy to prioritize and employ Navy security forces and capabilities in accordance with the Chief of Naval Operations' installation Required Operational Capabilities tiering system. The Required Operational Capabilities tiering system prioritizes installation physical security requirements according to the installation's operational missions as well as tenant and installation criticality. To support Required Operational Capabilities tiering system manning requirements, the Navy has implemented the Mission Profile Validation-Protection manpower model, which identifies the minimum manning required to set desired protection capabilities at each Navy installation. Per OPNAVINST 3300.53C, the Navy Antiterrorism Program, "All Navy installations or units owning a perimeter are required to possess a capability of self-defense as required in Force Protection Conditions Alpha and Bravo." Hence, this model identifies the minimum manning required to implement installation physical security requirements up to Force Protection Condition Bravo. To support physical security manpower requirements beyond Force Protection Condition Bravo, the Navy uses an Auxiliary Security Force model, which requires installation tenants and berthed ships to augment installation security forces with personnel trained to execute force protection watch standing requirements.

d. **Assessing Risk.** Department of Defense and Navy policy and guidance require commanders to conduct an annual security program assessment. Although details of the methodology used may vary amongst Fleet Commanders, use of certain elements is required including risk assessments, higher headquarters assessments and exercises. As part of this review, Commander, U.S. Fleet Forces polled Navy Regions and Fleet Commanders world-wide to ensure these required elements are used by all. Navy protection priorities and the resulting physical security posture are risk-based. Developing a current assessment of risk, required annually by the Department of Defense, involves consideration of three key elements--criticality, threat and vulnerability--as prescribed by Department of Defense Instruction 2000.16, "Department of Defense Antiterrorism Standards." Fleet Commanders leverage their latest risk assessments, which are informed by a determination and monitoring of the most likely and most dangerous threats to Navy assets, to manage vulnerabilities as part of a continuous assessment process.

e. **Assessing Adequacy and Alignment of Requirements.** Current physical security requirements are examined by Fleet Commander subject matter experts to assess how well those requirements set an effective defense-in-depth, in context with the specific threats identified by the most current risk assessment. In addition to examining adequacy of requirements, Fleet Commanders also ensure alignment with all higher headquarters guidance and directives. An effective defense-in-depth integrates specific physical security measures to optimize its capability to detect, assess, communicate, delay, deny and respond to the identified threats.

f. **Physical Security Assessments.** The current force protection assessment process, defined in Department of Defense Instruction 2000.16, Standards 6 and 31, mandates Higher Headquarters Program Reviews and outlines a triennial programmatic process to assess subordinate compliance with antiterrorism policies and standards. This triennial programmatic review cycle is comprised of an Integrated Vulnerability Assessment conducted by either the Naval Criminal Investigative Service or the Defense Threat Reduction Agency in year one; a higher headquarters antiterrorism program review conducted by the Navy Region in year two; and a self-assessed antiterrorism program review in year three. These reviews are compliance-based and administrative in nature--and while comprehensive, they do not evaluate a command's ability to execute the day-to-day antiterrorism mission.

In 2012, several antiterrorism-related incidents and improper security force responses prompted a U.S. Fleet Forces review of the antiterrorism capabilities of several installations. These installations had recently completed multiple Higher Headquarters Program Reviews and Assessments and were reported as being in compliance with governing antiterrorism guidance and policies. During these reviews, U.S. Fleet Forces noted capability and capacity gaps in day-to-day operations that current assessment protocols failed to identify. These gaps were identified when U.S. Fleet Forces observed and assessed demonstrations of installation antiterrorism responses to simulated threats.

To close this gap and ensure visibility into operational and tactical level force protection readiness, Commander, U.S. Fleet Forces directed the development of a formal process to assess the day-to-day operational capabilities of installations under his span of control. This led to the development of the U.S. Fleet Forces Higher Headquarters Antiterrorism Operational Assessment which was implemented in January, 2013. The U.S. Fleet Forces Higher Headquarters Antiterrorism Operational Assessment and Commander, Navy Installations Command Installation Protection Assessment Cell are specifically intended to evaluate operational vice administrative program execution. They are designed to verify tactical level understanding of Commander's Intent though demonstration and execution of pre-planned responses and watchstander level of knowledge reviews, and assess day-to-day operating capabilities and potential capacity shortfalls in areas of manning, training and equipping. During fiscal year 2013, 15 Higher Headquarters Antiterrorism Operational Assessments were conducted.

3. Report Methodology

This report answers each specified task detailed in the Secretary of the Navy's memorandum, "Base, Station, and Installation Physical Security Assessment," in a finding, discussion and recommendation format. The finding answers the specified task, followed by a discussion of the relevant, specific details to support the finding, followed by corresponding recommendations.

For Task 1, each finding is organized within the elements of Doctrine (Policy), Organization, Training, Material, Leadership, Personnel and Facilities (DOTMLPF). All major findings contained within this report are identified by bold text. All findings include a primary reference source--which is the basis for the finding (following the finding).

The findings under Task 1 apply equally to Task 6 and 11--accordingly the associated Task 1 findings, discussion and recommendations were not repeated in Tasks 6 and 11. In addition, the findings under Task 9 apply equally to Task 13--therefore, the findings, discussion and recommendations were not repeated.

4. Tasks, Findings, Discussion and Recommendations

Task 1. Identify any gaps in doctrine, organization, training, material, leadership and education, personnel and facilities (DOTMLPF) that affect security program execution.

Finding 1.1. (Doctrine/Policy-Major) The Navy's force protection program does not effectively connect the elements of assessment, readiness reporting and risk analysis to resourcing. *(Navy Inspector General Special Study on Antiterrorism and Force Protection, Findings 3 and 5)*

Discussion. The Navy's assessment process is vulnerability-centric with little emphasis on threat, criticality and installation force protection readiness. Consequently, a large number of vulnerabilities are catalogued, many of which remain uncorrected due to resourcing shortfalls. Additionally, information captured in the Defense Readiness Reporting System-Navy currently lacks installation readiness data and metric specificity. Improvement in Defense Readiness Reporting System-Navy reporting could be realized by development of specific metrics that are focused on consistent, verifiable and objective risk analysis criteria. Finally, Defense Readiness Reporting System-Navy Afloat does not have an Antiterrorism Force Protection capability area, such as exists for Navy Shore Installations, and the antiterrorism associated Navy Task Areas are spread across other warfare areas, masking actual antiterrorism readiness.

Recommendation 1.1.1. Establish an oversight process to review and assess installation force protection readiness based on all risk components including threat, vulnerability and criticality. Ensure assessment results are used in the Planning, Programming, Budgeting and Execution process and execution year resourcing plans.

Recommendation 1.1.2. Improve Defense Readiness Reporting System-Navy reporting to assist Commanders in quantifying risk, based on estimates of threat, criticality and vulnerability.

Recommendation 1.1.3. Establish Force Protection as a separate capability area in Defense Readiness Reporting System-Navy for afloat units and integrate with ashore units.

Finding 1.2. (Doctrine/Policy-Major) Prior to January, 2013, Navy force protection assessment processes focused exclusively on antiterrorism program administration and did not evaluate an installation's ability to operationally execute that program at the tactical level. *(U.S. Fleet Forces Command assessment site visits)*

Discussion. The current force protection assessment process, as delineated in the Department of Defense Instruction 2000.16 "Department of Defense Antiterrorism

Standards," is conducted on a triennial cycle, with an Integrated Vulnerability Assessment conducted in year one, a higher headquarters program review in year two, and a self-assessment in year three. These assessments use benchmarks developed by the Defense Threat Reduction Agency and are focused exclusively on the administrative components of the antiterrorism program. Consequently, there is no process to ensure installation security forces are able to operationally execute pre-planned responses at the tactical level. U.S. Fleet Forces and Commander, Navy Installations Command recognized this gap in the current assessment process and began development and execution of the U.S. Fleet Forces Higher Headquarters Antiterrorism Operational Assessment and the Commander, Navy Installations Command Installation Protection Assessment Cell, both of which are specifically designed to be an operational assessment of how well security forces execute at the tactical level.

Results from integrated vulnerability assessments and higher headquarters program reviews are entered into the Core Vulnerability Assessment Management Program, a computerized database. Although the U.S. Fleet Forces and Commander, Navy Installations Command staffs conduct quarterly reviews of Core Vulnerability Assessment Management Program data to ensure corrective actions are being completed, there's no systemic process by which the most senior leaders are periodically informed of outstanding deficiencies and potential operational risk. Additionally, although the decision to fund or not fund a particular corrective action is reviewed as part of the overall Navy programming cycle, any resultant risk is assumed by the operational commander under tactical control for force protection authority.

Recommendation 1.2.1. Continue development and implementation of the Higher Headquarters Antiterrorism Operational Assessment and Installation Protection Assessment Cell processes.

Recommendation 1.2.2. Develop a formal periodic feedback mechanism to ensure senior Fleet and installation enterprise leaders at the right level have visibility into deficiencies and vulnerabilities, and the status of associated corrective actions.

Finding 1.3. (Doctrine/Policy) Currently, only certain stand-alone off-installation Department of the Navy facilities receive regular higher headquarters antiterrorism assessments. A comprehensive review is necessary in order to determine stand-alone off-installation facility higher headquarters antiterrorism assessment requirements, periodicity and scope. *(Inspector General finding during command inspection of Commander, Navy Reserve Force, September 2013)*

Discussion. Stand-alone off-installation facilities that support Department of the Navy operations range from small office spaces in commercial buildings to large Navy Operational Support Centers. Additionally, some stand-alone activities contain support facilities that include Sensitive Compartmented Information Facilities, armories, communication equipment and combat support equipment. Acknowledging that stand-alone facilities vary in size, scope and activity, a comprehensive review will indicate which facilities require higher headquarters antiterrorism assessments and which facilities--that are limited in size and/or scope—do not require such outside assessments.

Recommendation 1.3. Conduct a comprehensive review of all stand-alone off-installation Department of the Navy facilities in order to determine which facilities require higher headquarters antiterrorism assessments, associated assessment requirements and assessment periodicity.

Finding 1.4. (Doctrine/Policy) Naval Criminal Investigative Service threat assessments are not site specific and lack granularity, which complicates the development of antiterrorism plans. *(Navy Inspector General Special Study on Antiterrorism and Force Protection, Finding 6)*

Discussion. Installations must review and incorporate annual threat information into antiterrorism plans. Threat information provided by the Naval Criminal Investigative Service Multiple Threat Alert Center tends to be geographically generic, versus site specific.

Recommendation 1.4. Deliver improved site specific local threat assessments to Navy Commanders and Commanding Officers with the granularity required to update antiterrorism Plans.

Finding 1.5. (Doctrine) Installation Antiterrorism Force Protection managers lack consistent verifiable methods to quantitatively estimate threat, vulnerability and criticality risk components. *(Navy Inspector General Special Study on Antiterrorism and Force Protection, Finding 7)*

Discussion. Although Navy Antiterrorism Force Protection managers are nominally versed in the components of risk, there is no standardized Navy installation risk analysis methodology to quantitatively estimate risk at the installation level. As such, risk estimates generated at the installation level tend to be more qualitative than quantitative due to lack of granularity of local threat estimates, vulnerability estimates that do not incorporate a local threat and criticality estimates that do not consider the redundancy effects from nearby Department of Defense assets. This subjectivity skews local risk estimates leading to sub-optimized antiterrorism plans, inaccurate Defense Readiness Reporting System-Navy readiness reporting and ultimately erroneous investment and/or resourcing decisions.

Recommendation 1.5. Develop and implement a method to optimize quantitative estimates of threat, criticality and vulnerability to improve antiterrorism plans, Defense

Readiness Reporting System-Navy reporting and investment decisions that filter down to the installation level.

Finding 1.6. (Doctrine) The term "installation," for purposes of complying with force protection requirements, is not universally defined, which creates confusion as Navy Operational Support Centers, Recruiting Stations, hospitals, etc. attempt to comply with directed force protection requirements. *(U.S. Fleet Forces Force Protection Baseline Review)*

Discussion. The term "installation" is essential to a determination of the appropriate actions a unit implements with respect to the setting specific Force Protection Condition measures.

Various publications define an installation, but do not establish if Navy Operational Support Centers, Recruiting Stations, or Navy Reserve Officer Training Corps units fall within this category. Specifically:

- Department of Defense Instruction 5200.8R (Physical Security Program) defines installations as "Real Department of Defense properties including bases, stations, forts (including National Guard and Federal Reserve Centers), depots, arsenals, plants (both contractor and government operated), hospitals, terminals, and other special mission facilities, as well as those used primarily for military purposes."
- Joint Publication 1-02 removed the definition for "installation" from the current edition. The previous edition's definition was "Installation--a grouping of facilities, located in the same vicinity, which support particular functions. Installations may be elements of a base."
- The current edition of Joint Publication 1-02 provides the following:

> Facility--a real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement, and underlying land. See also air facility.
>
> Base--1. A locality from which operations are projected or supported. 2. An area or locality containing installations which provide logistic or other support. 3. Home airfield or home carrier. See also base of operations facility.

Recommendation 1.6. Develop a consistent, Department of Defense-wide definition of "installation," so that all Commanding Officers have clear guidance for the implementation of Force Protection Condition measures.

Finding 1.7. (Organization-Major) The Navy's organizational construct with respect to its requirements and resourcing strategy for force protection adversely affects organizing (manning), training, equipping and operational execution. *(Navy Inspector General Special Study on Antiterrorism and Force Protection, Findings 1, 8 and 14; U.S. Fleet Forces Baseline Review; U.S. Fleet Forces Navy Antiterrorism Program Review)*

Discussion. The force protection mission cuts across all Type Commanders, Geographic Combatant Commanders and warfare area boundaries and, as a result, responsibility for its resourcing is spread out among numerous resource sponsors. Consequently, the Navy does not have an effective, integrated, prioritized resourcing strategy that ensures force protection resources are being directed to the areas that most effectively mitigate program-wide risk. Additionally, since no single resource sponsor is accountable for force protection risk, and force protection requirements compete for resources against warfare requirements for which resource sponsors have direct responsibility, funding designated for force protection requirements is frequently redirected to meet the needs of primary warfare area requirements. U.S. Fleet Forces, with input from all Fleet Commanders, creates an annual integrated, prioritized capabilities list to address force protection gaps and seams. This list is provided to resource sponsors to assist in prioritizing force protection resourcing in order to meet critical fleet resourcing priorities. However, since no single entity is charged with the responsibility to ensure these priorities are met, critical fleet force protection priorities may be underrepresented within the Planning, Programming, Budgeting and Execution cycle.

Recommendation 1.7. Establish a single, independent force protection resource sponsor, with the authority and responsibility to manage and fund all aspects of the Navy's force protection program.

Finding 1.8. (Organization-Major) The current command and control structure--with Commander, Navy Installations Command executing administrative control and Fleet Commanders executing tactical control for force protection--creates a seam between mission accountability (actual risk) and budgetary authority (programmatic risk). *(Navy Inspector General Special Study on Antiterrorism and Force Protection, Findings 2 and 13)*

Discussion. Current Navy organizational alignment separates ashore force protection mission and antiterrorism program authorities. Fleet Commanders manage and are accountable for force protection mission execution, but lack force protection budget authority. Commander, Navy Installations Command manages the ashore antiterrorism program and has Administrative Control of Navy Regions and installations, to include force protection budget submission and execution. Separating mission accountability from budget authority creates a situation where requirements are detailed by Fleet Commanders, but resourcing to accomplish those requirements is controlled by Commander, Navy Installations Command.

Recommendation 1.8. Align Echelon II ashore force protection resourcing and execution responsibilities.

Finding 1.9. (Organization-Major) The Navy does not optimally task-organize its security forces, nor does it provide security professionals (Master-at-Arms and Security Officers) the training, community management and career pipeline afforded by other Department of Defense services for their respective security professionals. *(Navy Inspector General Special Study on Antiterrorism and Force Protection, Finding 10)*

Discussion. The current organization of Navy security forces is dependent upon the command to which they are assigned, rather than the common tasking to which they perform. This lack of standardized task organization can sub-optimize unity of command and unity of effort and inhibit transfer of expertise as security are re-assigned from one command to another.

For the enlisted Master-at-Arms, there is no standardized security force training continuum beyond their time in Master-at-Arms "A" school; and their A-school, compared to other services, is much shorter at 6.5 weeks (versus up to 21 weeks for similar courses within the other services). For the security officer community, the Navy uses Limited Duty Officers to source and staff most of its security officer requirements throughout the Fleet. While this results in a seasoned, experienced Antiterrorism Force Protection leader, there is no empowered single point (community manager) for standardization of either training or certification tailored to meet afloat, ashore and/or expeditionary warfare capabilities--there is no single entity empowered to drive a community training continuum or community officer and enlisted career paths.

Recommendation 1.9.1. Develop a standardized task organization to optimize Navy Security Force unity of command and unity of effort.

Recommendation 1.9.2. Assess the Navy Master-at-Arms “A” School curriculum compared to other Services to determine if it is properly scoped--and correspondingly, of adequate length.

Recommendation 1.9.3. Establish a career pipeline for Navy Security Officers with clearly defined career training objectives based on formally identified training requirements established by the Fleet Commanders and Commander, Navy Installations Command.

Recommendation 1.9.4. Improve the community management of Master-at-Arms by providing more advanced training, and defining career progression goals that will better develop Navy Security Force professionalism and competence.

Finding 1.10. (Training-Major) The Navy small arms qualification program is not optimally aligned to post-9/11 force protection watch standing requirements and creates a process which places unnecessary burdens on commanders. *(U.S. Fleet Forces Force Protection Baseline Review)*

Discussion. U.S. Fleet Forces, in concert with other stakeholders, conducted an extensive review of current Navy Small Arms training and qualification requirements. Surveys were developed for both users and instructors to gain insight directly from the Fleet with regard to procedures, confidence in their training and recommendations for improving the Small Arms Program.

Site visits were conducted at 38 locations, to include local law enforcement agencies, Navy Regions and FBI Small Arms Training Centers. Each visit focused on best practices in training, curriculum, equipment and facilities.

A comprehensive review and analysis of the collected surveys and site visit data identified several areas of interest and overarching focus areas in the Small Arms Program.

- Standardized training prior to live fire is not conducted with requisite frequency or standardization across all commands or weapons types to develop satisfactory proficiency.
- Small Arms Marksmanship Instructors and Line Coaches lack the tools, procedures and training to identify and coach shooters in proper shooting techniques or correct shooter deficiencies.
- Small Arms Marksmanship Instructors assigned to units with Visit, Board, Search and Seizure teams are not qualified to conduct the Category IV courses of fire mandated for Visit, Board, Search and Seizure teams.
- Instructors are required to train personnel semi-annually on specific topics, but lack lesson plans designed to provide training standardization.
- Navy Security Forces and force protection watchstanders are not provided training to enhance proficiency after initial qualification. Once a watchstander is formally trained and qualified through the Navy Security Force Sentry Course, follow on training provides only sustainment of basic qualification.
- The scoring criterion for the sustainment course of fire requirement is lower than the minimal annual qualification score.
- Due to the lack of a standardized weapons qualification management system, Commanding Officers and higher echelons cannot accurately assess weapons qualification and Force Protection readiness status.
- The OPNAV 5512/2 “Authorization to Carry” card does not have a method to annotate sustainment or qualification dates.

- OPNAVINST 3591.1F authorizes Type Commanders to designate armed personnel in Categories I, II, III, or IV. This has resulted in force protection posts/watch stations being manned by various categories of armed personnel.
- Category II courses of fire are outdated and do not meet the needs of Navy Security Forces and force protection personnel to maintain a shoot and move proficiency level for current watch standing requirements. The crew served weapon course of fire is overly subjective and does not objectively measure accuracy.
- Dry fire has been shown to increase shooter proficiency and qualification rates, but is not consistently conducted at the unit level.
- Security watchstanders armed with both a rifle and a pistol are not trained on how to transition from their primary to their secondary weapon.
- The limited number of small arms training simulators--which are not Program of Record systems--lack adequate maintenance support and correspondingly have diminished readiness in support of unit level weapons training plans.

Recommendation 1.10.1. Determine the aggregate Navy demand for small arms ranges--and the capabilities of current ranges in place--and adjust Navy range capacity, as necessary.

Recommendation 1.10.2. Conduct a Limited Objective Experiment to determine the most advantageous capabilities of small arms simulators and to what extent their use may improve the Navy's Small Arms Training and Qualification Program.

Recommendation 1.10.3. Establish a small arms simulator program of record.

Recommendation 1.10.4. Revise small arms qualification criteria to define the required proficiency standard.

Recommendation 1.10.5. Research and identify a universal weapons electronic training and qualification system capable of maintaining each armed watchstander's weapons training and qualification throughout their career, as well as producing an input to the Defense Readiness Reporting System-Navy to give commands accurate readiness information.

Recommendation 1.10.6. Enhance Small Arms Instructor and Line Coach curricula and qualification to ensure Navy Security Forces and force protection watchstanders receive standardized fundamental training in practical shooting elements such as shoot and move, use of barricades, weak hand rifle and pistol shooting and transition from primary (rifle) to secondary (pistol). Include additional dry fire instruction and one-on-one coaching to provide immediate feedback.

Recommendation 1.10.7. Review current watchstander arming requirements to determine if the number of personnel requiring small arms proficiency can be reduced.

Recommendation 1.10.8. Qualify Navy Security Forces to specific OPNAVINST 3591 standards based on individual post requirements.
Recommendation 1.10.9. Adjust Non-Combat Expenditure Allocation to train Navy Security Forces based on the outcome of a Limited Objective Experiment in order to meet proficiency standards vice arbitrary minimum qualification standards.

Finding 1.11. (Training) Navy policy on Hostile Intent Determination training is not clear or properly resourced. Navy commands spend significant funds to purchase small arms trainers with Hostile Intent Determination capabilities; however, there is no program of record or standardized requirement for these simulators. *(U.S. Fleet Forces Force Protection Baseline Review)*

Discussion. In 2012, the Navy identified the need to improve the ability of individual watchstanders to execute Hostile Intent Determination. This effort centered on gap analysis encompassing established doctrine, supporting courses of instruction and certification procedures for the watchstander within the force protection watch structure. Gaps include:

- Some Hostile Intent Determination policy; tactics, techniques and procedures, and training and certification tools are not current or relevant.
- There is no standardized definition of Hostile Intent Determination proficiency and its implications relative to policy, doctrine, training curricula and certification.
- Employment of counter-material non-lethal weapons as force multipliers to facilitate evaluation of material threats is inconsistent.
- Entry-level curriculum for security personnel lacks lesson plan(s) that specifically address Hostile Intent Determination as a stand-alone procedure. Hostile Intent Determination associated skill sets are addressed in separate lesson plans, but lack cohesion and overall linkage to the execution of Hostile Intent Determination as a performance task.
- Hostile Intent Determination associated performance tasks lack consistency across Navy Security Operations Exercise Program scenarios specifically relating to the employment and evaluation of Hostile Intent Determination pre-planned responses against applicable threats. In addition, the scenarios are not aligned with the Fleet Exercise Program.
- Employment of non-lethal weapons capabilities at waterside fixed fighting positions is not required by policy.

Recommendation 1.11.1. Develop a Hostile Intent Determination implementation plan that will address the following operational focus areas: doctrine, policy, training, certification, training, equipment, sustainment and command culture.

Recommendation 1.11.2. Conduct a Limited Objective Experiment on Hostile Intent Determination proficiency standards and determine the tools and means to meet those standards.

Recommendation 1.11.3. Develop and include a separate Hostile Intent Determination tactics, techniques and procedures section in Chapter 7 (Methods and Techniques) of NTTP 3-07.2.1 (Antiterrorism) that will facilitate the determination of intent in a timely and accurate manner. Concurrently, develop supporting training plans and lesson guides to be incorporated in the force protection training curriculum.

Recommendation 1.11.4. Modify exercise scenarios to include an increased emphasis on Hostile Intent Determination as a stand-alone, performance-based, specified task.

Recommendation 1.11.5. Direct the operational requirement for, and subsequent redistribution/acquisition of, non-lethal weapons to enhance Hostile Intent Determination.

Recommendation 1.11.6. Conduct a review of all existing policy and instructions to direct the requirement for the use of non-lethal weapons to determine hostile Intent.

Recommendation 1.11.7. Determine effectiveness of current non-lethal weapons in shaping behavior and Hostile Intent Determination execution. Determine whether current systems are effective from ashore, afloat (Harbor Security Boats, as well as Navy combatants) and the waterfront. Additionally, determine if they have the capability to appropriately shape behavior, can effectively determine hostile intent, are easily used, are readily available and are effective. Include a cost-benefit analysis that will inform acquisition recommendations.

Finding 1.12. (Training) There is no requirement for integrated training between afloat, ashore and expeditionary security forces. *(U.S. Fleet Forces Force Protection Baseline Review)*

Discussion. Integrated security plans in Fleet Concentration Areas require dedicated and integrated training and exercise. Currently, afloat training is executed by the Fleet as part of the Fleet Readiness Training Plan but ashore training is a completely separate program administered through the Navy Region. Coordinating these two plans via the Fleet Scheduling Conference would permit afloat participation in some installation training events, making both events more realistic and useful. Additionally, executing more frequent, small scale exercises focused on ashore/afloat integration will improve Navy ability to execute cooperative defense.

Recommendation 1.12.1. Fund integrated Antiterrorism Force Protection exercises with afloat, ashore and expeditionary security forces, to include tenant commands and non-Navy stakeholders (local first responders). Fund Solid Curtain and Citadel Protect type exercises throughout the Future Years Defense Plan.

Recommendation 1.12.2. Consider establishing range facilities in Fleet Concentration Areas that incorporate live fire, simulation and simulated munitions into a single building design. Ensure new range construction provides live and simulated fire (including Crew Served Weapons training; Visit, Board, Search and Seizure; Secure Reaction Force; building search and clearing; and Close Quarters Combat capabilities) in an integrated training facility.

Recommendation 1.12.3. U.S. Fleet Forces submit to the Navy Staff defined requirements for integrated training between afloat, ashore and expeditionary security forces.

Finding 1.13. (Training) The Navy Antiterrorism Officer Level II training course curriculum is outdated. *(Navy Inspector General Special Study on Antiterrorism and Force Protection, Findings 12)*

Discussion. In its current form, Antiterrorism Officer Level II training does not adequately prepare individuals to assume Antiterrorism Officer duties and responsibilities with regard to antiterrorism planning, risk assessment or force protection reporting requirements. Additionally, almost all major Antiterrorism Force Protection instructions have been significantly revised since the Antiterrorism Officer Level II curriculum was written and many new and/or revised requirements are not captured in the current course.

Recommendation 1.13. Update the Antiterrorism Officer Level II training curriculum to include standard antiterrorism planning and address new requirements established since last time the curriculum was updated.

Finding 1.14. (Training) The inventory of personnel qualified as a Level II coxswain is not adequate to meet global Fleet manning requirements for Harbor Patrol Units. *(Navy Region input)*

Discussion. The only school house for training and qualifying Level II coxswains is via Naval Education and Training Command, Center for Security Forces at Joint Base Little Creek-Fort Story which has an annual throughput of 180 seats per year, of which 120 seats are dedicated to Commander, Navy Installations Command, 30 for Strategic

Systems Program and 30 for Navy Expeditionary Combat Command. As an example, Commander, Navy Installations Command requires 363 Harbor Patrol Unit coxswains to properly staff its Harbor Patrol capability. Several policy improvements with regards to classification of billets, increased recruiting, enhanced screening techniques and better detailing practices are already in progress and will significantly improve the Harbor Patrol Unit manning challenge in one to two years. Additional manpower and funding to expand the schoolhouse program by at least 40 more seats per year would accelerate the flow of Level II coxswains across the Fleet and help close the gap.

Recommendation 1.14. Assess options to increase the number of Level II coxswains in the Fleet.

Finding 1.15. (Training) Current Navy Security Force active shooter training is unrealistic and insufficient to best prepare for an active shooter/violent offender incident. (*Navy Region input*)

Discussion. Navy Security Force training involving weapons handling and reaction force tactics is limited--the current active shooter training regime lacks effective simulation to provide realistic training, and does not properly prepare security forces for an active shooter event. The Commander, Navy Installations Command active shooter response annual training requirement lacks sufficient periodicity to prepare Navy Security Forces for high risk active shooter response scenarios, nor is there a standardized or funded requirement for associated weapons training equipment.

Recommendation 1.15.1. Increase the periodicity requirement for active shooter response training and fund weapons feedback programs.

Recommendation 1.15.2. Assess options for developing and funding a weapons simulation device to improve installation active shooter response capabilities.

Finding 1.16. (Material) Life cycle management of Navy Security Forces equipment is not standardized. (*Navy Region input*)

Discussion. There is no standardized, overarching policy guidance on the determination, procurement and life cycle management of Navy Security Force equipment. For the most part, Type Commanders govern procurement of equipment, but efficiencies gained from economies of scale, standardization and management are not universally applied. Management of Navy Security Force equipment and antiterrorism systems for afloat forces is managed through a single Program Management Office (PMS-408)--this standardization has facilitated effective life-cycle management of equipment across multiple ship types and is resourced by the Navy Staff. This level of fidelity and standardization is not as refined across the other Budget Submitting Offices which employ Navy Security Forces. These inefficiencies reduce the effectiveness of individual and unit-level training and capabilities, interoperability and cost containment efforts.

Recommendation 1.16. Develop Echelon I-level policy that designates a Program Management Office charged with Navy Security Force equipment determination, standardization, life-cycle management and resourcing.

Finding 1.17. (Material) The Mission Profile Validation-Protection model does not address required administrative functions. *(U.S. Fleet Forces Force Protection Baseline Review)*
Discussion. The Mission Profile Validation-Protection model is focused on manning for security posts and does not address the full spectrum of security responsibilities. Consequently, there are not sufficient personnel to meet other core security requirements such as physical security surveys, annual publication reviews, installation antiterrorism exercises, training, records keeping and other routine administrative functions.

Recommendation 1.17. Modify the Mission Profile Validation-Protection manning model to ensure administrative and training functions are addressed.

Finding 1.18. (Personnel-Major) The Navy does not have sufficient organic escort capacity to meet the requirements of OPNAVINST 3380.5 "High Value Unit Transit Protection Operations." Although planning is in progress to close this gap, there is no dedicated funding programmed to support the High Value Unit escort mission. *(U.S. Fleet Forces Force Protection Baseline Review)*

Discussion. Historically, the U.S. Coast Guard has provided approximately 1,300 High Value Unit escort missions per year out of a total Navy requirement of 1,900. In October 2012, a U.S. Coast Guard memorandum stated that U.S. Coast Guard High Value Unit escort capacity would be reduced to 1,000 escorts in FY13 and 750 in FY14. In July 2013, the U.S. Coast Guard indicated that additional High Value Unit escort reductions would occur in FY15, specifically 450 escorts and across the board reductions in all Navy Fleet Concentration Areas with homeported High Value Units. Furthermore, U.S. Coast Guard expects to support approximately 100-150 annual High Value Unit escorts in non-Fleet Concentration Areas beyond FY15.

On October 1, 2013, Reserve Coastal Riverine Squadron Eight assumed the High Value Unit escort mission for Naval Submarine Base New London. This mission is funded for a single year (FY14) using an interim solution of Active Duty for Special Work--funds are not programmed for FY15 and beyond.

There is no Navy force structure identified, funded or trained to assume the continental United States-based High Value Unit escorts mission, although the identified interim solution using Reserve Coastal Riverine Forces may be an option in the long-term, if properly resourced.

Recommendation 1.18. Assess options and identify solutions to establish Navy High Value Unit transit escort capability for FY15 and beyond.

Finding 1.19. (Personnel-Major) For installations within the continental United States, security forces are currently manned at less than 80 percent of the validated requirement. *(U.S. Fleet Forces Force Protection Baseline Review)*

Discussion. Following the October, 2000 terrorist attack against USS COLE, the Navy authorized and funded significant increases in its military, civilian and contractor security forces.

As installation security requirements stabilized in 2007 and 2008, the Navy recognized a new strategy was necessary to balance military, civilian, foreign national and contractor personnel security forces. In 2008, guard functions were reassessed based on installation assets and capabilities, geographic size and population the of installation, and historical analysis of local crime and threats. Additionally, in 2008, Congress directed the Navy to commence a phased drawdown and elimination in 2012 of all post-9/11 contract guards--representing ten percent of the total security force at that time. In 2009, non-guard functions, under the results of an Office of Management and Budget A-76 Standard Study, were converted from mostly military personnel to civilian. In 2011, conversion from contractor to government civilians began in order to comply with the congressionally mandated drawdown. Later in 2011, the Office of Secretary of Defense directed a Service-wide civilian personnel ceiling of “not greater than 2010 levels”--which affected both the Navy security contractor-to-civilian conversion initiative and the overall size of the Navy civilian law enforcement community, such that a Reduction in Force for Navy civilian law enforcement personnel would be required by January 1, 2014.

The sum total effect of this combination of law, policy and funding decisions is that the current ashore activities’ security workforce is funded (after January 1, 2014) to only 81 percent of Mission Profile Validation-Protection manning model requirements--which will result in manning at only 75 percent of the requirement due to funding, training lead times, hiring process delays and personnel unavailable for duty. To establish security force manning requirements, the Navy uses the Mission Profile Validation-Protection manpower model, which identifies the minimum manning required to set desired protection capabilities at each Navy installation up to Force Protection Condition Bravo. To support physical security manpower requirements beyond Force Protection Condition Bravo, the Navy uses an Auxiliary Security Force model, which requires installation tenants and berthed ships to augment installation security forces with personnel trained to execute force protection watch standing requirements.

To mitigate this systemic manpower and manning shortfall, installation commanding officers have few options to mitigate the gap between on board manning and the Mission Profile Validation-Protection requirement. Funds for overtime of civilian security force personnel are extremely limited and normally available only during extraordinary contingencies. Memorandums of Agreement with local, state or federal agencies are typically focused on highly specialized skill sets which organic installation forces may lack. Accordingly, installation security departments are forced to extend active duty military personnel working hours. However, this effort cannot be sustained indefinitely without directly affecting unit morale and training sustainment required to maintain proficient watchstanders. Installation security departments routinely leverage their Navy Reserve security forces, but by design and funding this is a surge work force that can be recalled full-time only during an extended national emergency. Additionally, as noted above, installation commanding officers are authorized to direct their on-installation tenant commands to provide a portion of their military personnel to serve as Auxiliary Security Forces. Installations with very few or no military tenant commands have no Auxiliary Security Force-eligible personnel to draw from and, therefore, must extend the working hours of assigned military personnel, increase use of Navy Reserve forces and/or curtail security services.

For installations located outside of the continental United States, options available to installation commanding officers may be more limited. Some locations have little to no Auxiliary Security Force from which to augment organic security forces. Navy Reserve security force units dedicated to those locations are located in the continental United States and cannot be easily leveraged to augment installation security forces--and funding for temporarily recalled Navy Reserve security forces is significantly constrained. Additionally, use of civilian security guards or contract security forces may be limited by the dictates of the governing Status of Forces Agreement or host nation law. Accordingly, the only option available at these locations to make up for undermanned security forces is to extend working hours for organic security forces or curtail security services.

As discussed previously, budget constraints have resulted in current and projected security force manpower/manning that do not meet Mission Profile Validation-Protection requirements. Contributing to this, U.S. Fleet Forces has identified at least 407 Master-at-Arms billets that are not aligned with Fleet force protection priorities. The current manpower shortage requires installation commanders to use Auxiliary Security Forces to meet Force Protection Condition Alpha security requirements--our current 24/7 baseline. While trained satisfactorily for the mission, Auxiliary Security Forces do not possess the same level of experience and skill as full-time security forces. Additionally, to make up for a shortage of trained installation security forces, shipboard personnel are frequently required to man pier Entry Control Points. Some installations are manned solely by civilians and do not have an Auxiliary Security Force pool to draw from. This results in the installation having to close entry control points in order to comply with security requirements.

Finally, at some installations, resource reductions make hands-on training difficult to accomplish. Sustainment training at some installations is relegated to computer based training. Furthermore, as manpower and funding are reduced, installations are unable to assemble a watch section dedicated to training--consequently, real world watchstanders are participating in training evolutions. Although this is an efficient use of time and resources, this practice is less effective and has potentially significant safety and security implications. Additionally, training is not as realistic as desired.
Recommendation 1.19.1. Man installation security departments to Mission Profile Validation-Protection requirements.

Recommendation 1.19.2. Relocate Master-at-Arms serving in identified misaligned billets to those where they provide the most effective and efficient readiness and capability.

Recommendation 1.19.3. Review ashore tenant command security requirements. Realign redundant security forces across the force and/or conduct a budget based transfer from the tenant command to the installation security department.

Finding 1.20. (Personnel-Major) The Mission Profile Validation-Protection model does not account for limited duty or otherwise not "Fit for Full Duty" Navy Security Force personnel. *(Navy Inspector General Special Study on Antiterrorism and Force Protection, Finding 11)*

Discussion. Navy Total Force Manpower Policies And Procedures, OPNAVINST 1000.16K, and the Mission Profile Validation-Protection requirements determination model formulas do not allow for projecting limited duty or otherwise not fit for duty rates in determining the productive work week factor in the model. The model is exclusively built assuming 100 percent funding of the manpower requirement and that there is subsequent 100 percent manning to the requirement. Any degradation in either manpower or manning below the Mission Profile Validation-Protection standard incurs operational risk, requiring installation commanding officers to triage the shortfall via watch bill management, leave approval, Auxiliary Security Force use, cross-training and additional sustainment training. Reduced security force manning results in longer working hours for Sailors, frequently leaving time and resources to sustain only minimum qualifications in assigned watch stations. The only exception in the Navy security force community to this policy is at nuclear weapons sites where their model allows them to be funded and manned at 120 percent of their requirement due to a historical 20 percent non-Personnel Reliability Program compliance rate.

Recommendation 1.20. Determine additional manpower required and impacts to global manning distribution if installations were manned at 105-110 percent of the Mission Profile Validation-Protection requirement.

Finding 1.21. (Personnel) There are no funded Antiterrorism Officer positions at the installation level. *(U.S. Fleet Forces Force Protection Baseline Review)*

Discussion. Department of Defense Instruction 2000.16 and OPNAVINST F3300.53C both direct that an Antiterrorism officer be designated, in writing, for each installation. Additionally, NTTP Antiterrorism 3-07.2.1 states that the Antiterrorism Officer is "the primary advisor to the commanding officer." The Antiterrorism Officer is the installation commanding officer's subject matter expert on the Navy's Antiterrorism Program.

While neither the Department of Defense Instruction 2000.16 or OPNAVINST F3300.53C direct that the Antiterrorism Officer position must be a full-time duty position at the installation level, due to the scale and complexity of large Navy installations, assignment as a full-time duty position may be warranted. Currently, at many Navy installations, the Antiterrorism Officer position is assigned as a collateral duty--most frequently to the installation security officer. At large Navy installations, the primary duties of the installation security officer are comparable to those of a police chief of a small city--managing, training, and directing the installation's security force. Accordingly, assignment of Antiterrorism Officer duties to the installation security officer as a collateral duty, particularly at large Navy installations, can easily lead to the duties of this critical position not being afforded a sufficient level of attention for proper execution of the installation Antiterrorism Program.

Assignment of the Antiterrorism Officer position as a collateral duty could potentially create a conflict of interest where the realities of resource constrained day-to-day security operations compete with Antiterrorism Program requirements--leading to a situation where the installation commanding officer may not be fully informed of Antiterrorism Program deficiencies. In addition, the installation security officer is normally subordinate to the operations officer, and therefore does not report directly to the commanding officer in the execution of his primary duties--which may inhibit his access to the commanding officer in the execution of his collaterally assigned duty as Antiterrorism Officer.

Recommendation 1.21. Resource full-time Antiterrorism Officers billets at the installation level, as appropriate, based on antiterrorism program size and complexity.

Task 2. Validate procedures by which Commanding Officers determine the degree of contractor access to government installations and facilities.

Finding 2.1. Commander, Navy Installations Command physical access control processes used by Installation Commanding Officers to determine the degree of contractor access to government installations comply with the requirements established in Homeland Security Presidential Directive 12, Secretary of Defense Directive Type Memorandum 09-012 and Department of Defense 5200.08-R Physical Security Program. (*Commander, Navy Installations Command input*)

Discussion. Commander, Navy Installations Command issues contractor access credentials and performs background screening based on the type of access required. If a contractor requires logical access, which is access to Information Technology systems, that contractor is issued a Department of Defense Common Access Card with background screening conducted through a National Agency Check with Inquiries. If a contractor requires only physical access to the installation, then Commander, Navy Installations Command issues a Navy Commercial Access Credential System credential. Prior to issuing a Navy Commercial Access Credential System credential, installation personnel appointed by the installation Commanding Officer vet the contractor through the National Crime Information Center and Terrorist Screening Databases. Additionally, the Navy Commercial Access Credential System commercial credentialing provider reviews additional federal, state and local records checks

The Navy Physical Access Control Program which includes Navy Commercial Access Credential System, is a mutli-year project to fully implement the Secretary of Defense's Directive Type Memorandum 09-012 requirements--Secretary of Defense Directive Type Memorandum 09-012 is an unfunded mandate, which directs implementation as "resources and law allows." Commander, Navy Installations Command has an ongoing, proactive management team in place to oversee the implementation of the policy/program and to address compliance challenges as they are identified.

Contractors whose background vetting indicates felony convictions are denied installation access. Applicants may request a waiver for access from the installation Commanding Officer, who will make the waiver determination based on Commander, Navy Installations Command access control requirements as delineated in CNICINST 5530.14A. The seriousness of the offense and time since the felony conviction(s) are the primary considerations used in the waiver adjudication process.

Recommendation 2.1. Commander, Navy Installations Command continue to use the access control processes described above for contractors.

Task 3. Examine procedures used in the Continuous Evaluation Program and uniform standards of compliance.

Finding 3.1. The Continuous Evaluation Program as currently constructed in policy is not effective in preventing security leaks, espionage and kinetic events in the work place. *(Naval Criminal Investigative Service input*)

Discussion. The SECNAVINST M-5510.30 DoN Personnel Security Program directs all commands to have a Continuous Evaluation program. Under the guidelines of this program, personnel are required to report themselves, coworkers are required to report their coworkers and supervisors are required to monitor their subordinates. Real world experience has shown that the threshold at which an individual exhibits behavior aberrant enough to warrant intervention by his coworkers or supervisors is above the level of behavior that may actually be indicative of real risk--particularly when evaluated during post-incident forensics.

In general, Navy workers trust each other, and work in an environment where people are disinclined to report each other. Many behavioral factors may lead to a reluctance to report each other, including (1) What happens if I'm wrong, (2) This could ruin his/her career, (3) I could be held liable, (4) Someone else will notice and take care of it. These same factors often delay or prevent the reporting of inappropriate behavior in the sexual assault arena, and are associated with a societal aversion to potentially impinge upon the rights of a co-worker unless their actions have a direct detrimental effect on ourselves.

Recommendation 3.1.1. Evaluate the necessity to update SECNAVINST M-5510.30 to include behavioral indicators of potential violent actors to be reported in accordance with the Continuous Evaluation Program.

Recommendation 3.1.2. Develop an automated system for Continuous Evaluation Program that is linked to the Joint Personnel Adjudicated System to enable expeditious evaluation with respect to security clearance impact.

Recommendation 3.1.3. Better publicize the Naval Criminal Investigative Service Threat Management Unit capabilities to evaluate and pursue reported personnel and issues.

Recommendation 3.1.4. Consider developing a Navy-wide training program that sensitizes the force to the issues surrounding espionage, leaks, work place violence and mental health monitoring and how we expect the work force to react.

Task 4. Review Service access control policy and procedures and risk mitigation measures.

Finding 4.1. Navy physical security access control policies and procedures are adequate and aligned with higher headquarters. (*U.S. Fleet Forces Base, Station, and Installation Physical Security Review-Part 1*)

Discussion. Subject matter experts examined Navy physical security directives and guidance to ensure that current policy requirements establish a defense-in-depth through the employment of detect, assess, communicate, delay, deny and respond capabilities. Within the past year, U.S. Fleet Forces conducted a Force Protection Baseline review that included more than 50 physical security subject matter experts to examine 63 distinct threat-asset pairs to assess the adequacy of current force protection requirements.

This assessment verified that current policy requirements are adequate to establish an effective force protection posture, given the currently assessed risk. Additionally, during this assessment, all Fleet Commander physical security directives were examined and found to be in alignment with Department of Defense, Secretary of the Navy, Chief of Naval Operations and Geographic Combatant Commander guidance.

Recommendation 4.1. Continue routine review of Navy physical security access control policies and procedures to ensure adequacy and alignment.

Finding 4.2. Navy physical security doctrine focuses on mitigation of the most likely and most dangerous threats to assets and personnel rather than that of postulated threats. (*USFF Base, Station, and Installation Physical Security Review-Part 1*)

Discussion. The Navy's current force protection methodology assesses risk against the most likely and most dangerous threats, as determined by Naval Criminal Investigative Service Multiple Threat Alert Center and the broader intelligence community. Consequently, some postulated threats (e.g., swimmer or light aircraft), although considered in the risk assessment process, may not be mitigated at every location. Attempting to mitigate every low probability or relatively inconsequential threat for a given Area of Responsibility would not only be ineffective, but would incur substantial cost for a very low return on investment with respect to the mitigation of potential risk. However, dependent upon the location of an installation and the credibility of specific threat data, Geographic Combatant Commanders will modify the baseline force protection posture to ensure additional threats are mitigated based on threat probability or consequence.

Recommendation 4.2. Continue to ensure adequate mitigation of most likely and most dangerous threats to Navy assets and personnel, while considering postulated threats during the conduct of periodic risk assessments.

Task 5. Review Installation Command and tenant Command/Activity security procedures and supported/supporting relationships.

Finding 5.1. Mutual Support and Immediate Response Agreements are an exceptionally valuable element of an installation's response capability. *(Commander, Navy Installations Command input)*

Discussion. Over time, regions and installations have developed Mutual Support and Immediate Response Agreements to support and supplement mission requirements on board the installation and to provide support to civilian authorities outside the installation. These agreements are directed by and constructed in accordance with existing service and program policy. Some common examples of Mutual Support and Immediate Response Agreements include fire and emergency services, supplementary security and/or Special Weapons and Tactics capability, and Explosive Ordnance Disposal.

The need to have a full suite of functional Mutual Support and Immediate Response Agreements to supplement installation capability is even more critical as an element necessary to ensure installation mission sustainment. In particular, the forces and capabilities provided by Mutual Support and Immediate Response Agreements are most critical during mass conflagration events.

Recommendation 5.1. Direct all installations to develop Mutual Support and Immediate Response Agreements with local, city, county, state, or other federal authorities and agencies in order to better meet potential response requirements.

Finding 5.2. Regions and Installations routinely exercise emergency management and antiterrorism plans. However, involvement by and integration of tenants into those exercises varies widely throughout the ashore enterprise. (*Commander, Navy Installations Command input*)

Discussion. Tenants on Navy installations rely on the host installations they are located aboard for antiterrorism security and emergency management support. While nearly all the programmed capability for these key installation missions comes from the installation, the degree of involvement, cooperation and compliance of tenants during actual events significantly affects the successful outcome of the event.

The authorities assigned to region and installation commanders in Navy Regulations gives those commanders authority to direct the actions of installation tenants during antiterrorism and emergency management events. Integration and coordination of the installation and tenant antiterrorism and emergency management activities is directed in Navy doctrine and policy. Installation commanders can also direct tenant involvement in preparatory planning and training exercises. Exercising that implied authority is viewed as essential to success by the region/installation commanders, including involvement in installation antiterrorism and emergency management exercises and planning.

Recommendation 5.2.1. Develop and publish Echelon I policy that lays out in detail the full scope of required relationships and obligations between tenants and the installation commander.

Recommendation 5.2.2. Expand the ashore exercise planning and assessment processes to evaluate all tenant involvement, participation and compliance with installation antiterrorism and emergency management requirements, particularly with respect to what may be assessed as the most dangerous and most likely antiterrorism and emergency management potential scenarios.

Finding 5.3. Existing antiterrorism orders, doctrine and policy require Navy Security Forces to be fully integrated within each Commanding Officer's operational environment. While afloat units (and their security capabilities) are fully integrated into installation antiterrorism/security organizations, the separate armed security forces employed by some installation tenants are not similarly integrated in to the larger installation antiterrorism/security force. (*Commander, Navy Installations Command input*)

Discussion. On board certain installations, some tenant commands employ their own separate armed security forces (most often contractors) to supplement the existing security umbrella provided by installation Navy Security Forces. This action (unless specifically approved) is contrary to Chief of Naval Operations policy (OPNAVINST 5530.14E), and adversely challenges unity of command and unity of effort. Additionally, there is no process in place to ensure that both installation and tenant procured security forces are fully integrated, trained and equipped to the same standards.

Recommendation 5.3. Conduct a review of existing tenant specific security forces to ensure they are necessary in accordance with service doctrine and policy. Consider making those forces part of the Mission Profile Validation-Protection team for the host installation, and transferring those forces to the installation Commanding Officer.

Task 6. Review requirements, resources and priorities for security encompassing infrastructure enhancement, access control, law enforcement, military police and information/personnel security manpower.

In responding to Task 1, we reviewed requirements, resources, and priorities for security encompassing infrastructure enhancement, access control, law enforcement, military police and information/personnel security manpower.

Task 7. Identify technology enhancement options to mitigate risk and offset resource shortfalls.

Finding 7.1. Commander, Navy Installations Command has developed an enterprise approach to conduct credential verification using technology solutions to improve physical security and access control. (*Commander, Navy Installations Command input*)

Discussion. Access control to installations and facilities is one of the most effective ways to deter potential perpetrators, but also one of the most challenging to execute on a day-to-day basis. The Navy relies upon accurate vetting and credentialing of personnel, but this is process is only as effective as the ability to access databases in real time to conduct accurate verification of credentials prior to granting access. Improved technology provides instant access to conduct background checks and make informed decisions regarding access. Commander, Navy Installations Command's enterprise physical access control solution includes applications, infrastructure, pedestrian turnstiles, gates, hand held scanners, hardware and software. Additionally, Commander, Navy Installations Command has developed/initiated the following technology enhancements:

- Public Safety Network (PSNET)/Enabler. Commander, Navy Installations Command is in the process of providing connectivity to installation entry control points through Public Safety Network. Using the Enabler middleware system, Commander, Navy Installations Command will be able to electronically scan Common Access Cards, Navy Commercial Access Control System cards and other government issued credentials to conduct personal identity verification.
- Navy Commercial Access Control System. Standardizes and enhances vetting for non- Common Access Card eligible contractors requiring physical access to Commander, Navy Installations Command installations.
- Automated Vehicle Gates. Commander, Navy Installations Command is in the process of installing Automated Vehicle Gates at selected entry control points across the enterprise. These gates will provide automated access control while reducing entry control point manpower requirements. Automated access control will be conducted using Public Safety Network/Enabler.

Recommendation 7.1. Support continued implementation of Commander, Navy Installations Command's enterprise physical access control initiatives and assess the feasibility of increasing the frequency of Navy Commercial Access Control System database updates.

Finding 7.2. Commander, Navy Installations Command has developed a metric-based decision making capability to mitigate risk and optimize use of available resources. (*Commander, Navy Installations Command input*)

Discussion. The following decision making models have been developed:

- Mission Profile Validation-Protection. This metric based model standardizes manpower requirements for security forces across the Commander, Navy Installations Command enterprise.
- Risk Informed Investment Strategy. A risk based model that provides decision making metrics for antiterrorism resourcing across the Commander, Navy Installations Command enterprise.
- Protection Program Objective Memorandum. A tool that addresses budget projections and application strategy to develop protection program funding solutions across the Commander, Navy Installations Command enterprise.
- Data Housing and Automated Reporting Tool. Provides training metrics, identifies gaps and forecasts needed training requirements for Commander, Navy Installations Command personnel.

Recommendation 7.2. Continue to investigate and pursue funding for technology solutions to mitigate risk and optimize use of available resources to mitigate shortfalls.

Task 8. Evaluate training and education programs to identify contributing factors and behavioral indicators of potentially violent actors, and to increase commander awareness of the need for continuous evaluation.

Finding 8.1. Installation commanders are not fully leveraging Naval Criminal Investigative Service support in order to potentially identify violent actors and increase awareness of the insider threat. *(Naval Criminal Investigative Service input)*

Discussion. The Naval Criminal Investigative Service provides ongoing support to Navy installations through their Threat Mitigation Unit and Security Training Assistance and Training Team. These Department of the Navy resources increase the installation commander's capability to potentially identify "contributing factors and behavioral indicators," as well as having a well-trained response force.

The Naval Criminal Investigative Service Headquarters Threat Management Unit supplies training material for the quarterly Crime Reduction Campaign briefing related to workplace violence which is disseminated Navy-wide. This information entails an explanation of the violence process and pathway, violence myths, threat enhancers and a variety of concerning behaviors (verbal, non-verbal, physical and cues). Additionally, the briefing discusses the need for immediate reporting and offers multiple avenues in which to do so. The Naval Criminal Investigative Service Headquarters Threat Management Unit works in concert with Naval Criminal Investigative Service Insider Threat Program cases where there is a risk for future violence, as the definition of insider threat includes the potential for violent acts. The Naval Criminal Investigative Service Headquarters Threat Management Unit serves primarily in an operational capacity, providing pro-active investigative guidance and expertise to the field, pre-incident, based upon reported indications. Additionally, the Naval Criminal Investigative Service Headquarters Threat Management Unit provides advanced training to Naval Criminal Investigative Service field agents on threat assessment fundamentals.

The Naval Criminal Investigative Service Security Training Assistance and Training Team Program provides the Navy support in the areas of physical security assistance reviews, as well as routine Naval Security Force response training. Historically, Navy Security Force programs have received training in active shooter response, Non-Lethal Weapons Instructor, surveillance and counter-surveillance for security forces and security first responder training.

Recommendation 8.1. Continue to improve and use the Naval Criminal Investigative Service's multiple resources to expand the commanders' ability to provide continuous workplace monitoring of potential threats of workplace violence and, when necessary, effectively mitigate those threats.

Finding 8.2. The Naval Criminal Investigative Service provides annual Counterintelligence and Insider Threat Awareness and Reporting training, which includes education on the threats of espionage, terrorism, workplace violence and inadvertent threats to Navy and Marine Corps active duty and government civilians. *(Naval Criminal Investigative Service input)*

Discussion. The Naval Criminal Investigative Service provides training and briefings on guidance and procedures to increase the awareness of indications and warnings of possible precursors to violent acts. Additionally, this training details the reporting process to be used to provide precursor information to Naval Criminal Investigative Service for assessment, evaluation and action. This annual training is provided Navy and Marine Corps-wide by Naval Criminal Investigative Service agents in a live briefing format. Naval Criminal Investigative Service training is designed to help reduce the potential for violence in the work place, identify methodologies of adversaries to recruit trusted insiders, indicators of insider threat behavior and reporting requirements and methodologies. This training is an annual requirement for all Navy and Marine Corps active duty and government civilians.

Recommendation 8.2.1. Review and update, as necessary, Naval Criminal Investigative Service awareness materials to incorporate the latest findings from recent incidents in accordance with SECNAV instruction 5510.37.

Recommendation 8.2.2. Re-emphasize, at all levels, the importance of Naval Criminal Investigative Service training in order to identify and mitigate potentially violent actors.

Recommendation 8.2.3. Require contractors on government sites or who regularly require access to Navy-owned work spaces to receive annual Naval Criminal Investigative Service Counterintelligence and Insider Threat Awareness and Reporting training.

Task 9. Review personal weapons policies and procedures for uniformity and enforcement.

Finding 9.1. Procedures to control, possess and stow personal firearms on Navy installations are in place and effective. Navy installations are in conformance with the published Navy and Commander, Navy Installations Command instructions in effect in this area. (*Commander, Navy Installations Command input*)

Discussion. OPNAVINST 5530.14E (Navy Physical Security and Law Enforcement Program) and CNICINST 5530.14A (Commander, Navy Installations Command Ashore Protection Program) provide the detailed requirements for installation commanding officers to control personal firearms on their installations. Generally, the instructions require the installation commanding officer to grant permission to bring personal firearms on board in writing, and the instructions further detail the safety, security and handling requirements required when such permission is granted.

The principal variation within the ashore enterprise with respect to personal firearms on an installation is whether, when the Commanding Officer grants permission, personal weapons are permitted in the service members' quarters, or must be stored in the installation armory. This variation is permitted within the current policy, and allows the individual installation commanding officer the flexibility to ensure that the personal weapons are stored in a manner consistent with the particular population, armory capacity, size and housing environment of the installation.

Enforcement is accomplished by notification/signage at installation entrances and by publication/promulgation of CNICINST 5530.14A requirements that implement overarching OPNAVINST 5530.14E policy. Violations, when encountered, are processed through normal disciplinary channels in order to hold violators accountable.

Recommendation 9.1. Continue to comply with all Navy personal weapons policies and procedures.

Task 10. Assess the adequacy of current physical security doctrine to mitigate postulated threats.

Finding 10.1. Navy physical security doctrine focuses on mitigation of the most likely and most dangerous threats to assets and personnel rather than that of postulated threats. (*U.S. Fleet Forces Force Protection Baseline Review)*

Discussion. The Navy's current force protection methodology assesses risk against the most likely and most dangerous threats, as determined by Naval Criminal Investigative Service Multiple Threat Alert Center and the broader intelligence community. Consequently, some postulated threats (e.g., swimmer or light aircraft), although considered in the risk assessment process, may not be mitigated at every location. Attempting to mitigate every low probability or relatively inconsequential threat for a given Area of Responsibility would not only be ineffective, but would incur substantial cost for a very low return on investment with respect to the mitigation of potential risk. However, dependent upon the location of an installation and the credibility of specific threat data, Geographic Combatant Commanders will modify the baseline force protection posture to ensure additional threats are mitigated based on threat probability or consequence.

Recommendation 10.1. Continue to ensure adequate mitigation of most likely and most dangerous threats to Navy assets and personnel, while considering postulated threats during the conduct of periodic risk assessments.

Task 11. Identify barriers to physical security and access control policy implementation.

In responding to Task 1, we identified barriers to physical security and access control policy implementation.

Task 12. Recommend enhancements, improvements and innovations, if any, in procedures or policies that could improve our ability to provide security at our installations.

Finding 12.1. The Navy has not fully investigated the use of technology to assist in the identification of potential insider threats prior to an event occurring. *(U.S. Fleet Forces finding)*

Discussion. Recent high-profile incidents highlight the need to actively and continuously detect, deter and mitigate threats from those that have been granted access to our installations and facilities. Loss of life, damage to equipment and loss of classified data are clear examples of the danger posed by insider threats that may be deterred if potential perpetrators are identified early.

Recommendation 12.1. Leverage the Deputy Assistant Secretary of Defense for Nuclear Matters' Physical Security Enterprise and Analysis Group, and the Office of Naval Research, to explore technology solutions that could screen and identify potential insider threats to security.

Finding 12.2. The Department of Defense does not possess an automated system for the execution of the Continuous Evaluation Program. *(Deputy Under-Secretary of the Navy Plans, Policy, Operations, and Integration Input)*

Discussion. One of the noted weaknesses in the current security clearance program is the reliance on personnel to formally note and inform their leadership of potential aberrant behavior of co-workers. An automated system could leverage current societal social media expertise by using a web-based system to inform leadership of potential indicators, while maintaining a certain amount of anonymity--thereby reducing the potential stigma associated with informing on a co-worker. Additionally, this automated system could be linked to the Joint Personnel Adjudication System to ensure any noted aberrant behavior is acted upon in a timely manner.

Recommendation 12.2. Identify and implement potential systems that may be leveraged to automate the Continuous Evaluation Program.

Task 13. Assess current procedures to control, possess and stow personal firearms on installations in accordance with applicable law, while considering practical implications of effective implementation.

In responding to Task 9, we assessed current procedures to control, possess and stow personal firearms on installations in accordance with applicable law, while considering practical implications of effective implementation.

Task 14. Review the vetting and credentialing procedures within the Department of the Navy for base access and eligibility for security clearances while considering vetting and credentialing in the context of the broader Department of Defense procedures.

Finding 14.1. The Navy's vetting and credentialing procedures used for base access and security clearances by the Department of the Navy are in accordance with Department of Defense policy and directives. *(Deputy Under-Secretary of the Navy for Plans, Policy, Operations, and Integration input)*

Discussion. Vetting and credentialing of individuals requiring access to Department of the Navy installations and facilities falls into two primary categories--recurring or non-recurring. Non-recurring access is granted at the installation or facility according to installation commanding officer guidelines and involves simple vetting of personal credentials (e.g., driver's license) by means of a National Crime Information Center check. If no problems are determined as a result of the National Crime Information Center, a one-day pass is issued for installation access.

For recurring access to Navy installations and facilities the issuance of Common Access Cards, Navy Commercial Access Control System or TESLIN credentials are required. Specifically:

Common Access Cards for Department of Defense personnel and supporting contractors.

- Common Access Cards are issued to Uniformed Services personnel, Department of Defense civilian employees, and eligible contractor personnel.
- Common Access Cards are also issued to other eligible populations. These include non-Department of Defense federal civilians, state employees, and other non-Department of Defense affiliates who require physical access to facilities and/or logical access to Department of Defense networks and have a Department of Defense sponsor. Common Access Card eligibility for non-U.S. persons is based on Department of Defense government sponsorship. In order for a non-U.S. person to be issued a Common Access Card they must meet the following: legal residence in the U.S. for a minimum of three years, a positive result from a Federal Bureau of Investigation fingerprint check, an initiated National Agency Check with Inquiries or equivalent, and a successfully adjudicated National Agency Check with Inquiries as listed in the Under Secretary of Defense Directive Type Memorandum 08-003. A Common Access Card can only be issued after receipt of a favorable Federal Bureau of Investigation fingerprint check, per BUPERSINST 1750.10C.

- The Navy does not issue Common Access Cards to contractors unless they need both physical and logical access.

Navy Commercial Access Control System for contractors.

- Navy Commercial Access Control System credentials are issued to contractor personnel who are not Common Access Card eligible but require routine access to installations in the execution of their work to support the Navy.
- The Navy Commercial Access Control System provides a compliant, tamper resistant credential that can be electronically authenticated against authoritative databases.
- References and requirements regarding the issuance of Navy Commercial Access Control System credentials include Secretary of Defense Directive Type Memorandum 09-012 "Minimum Standards for Access Control," Department of Defense Instruction 5200.08-R Physical Security Program, Department of Defense Chief Information Officer Memorandum “Department of Defense Acceptance and Use of Personal Identity Verification-Interoperable (PIV-I)” dated October 5, 2010, and Department of Defense Chief Information Officer Memorandum “Department of Defense Requirements for Accepting Non-Federally Issued Identity Credentials” dated January 24, 2013.
- All non-Federally Issued Navy Commercial Access Control System credentials require minimum vetting by means of a National Crime Information Center, Terrorist Screening Database, and a Secretary of the Navy Memorandum/ OPNAVINST 5530.14 required Sexual Offender Registry check--and per the Secretary of Defense Directive Type Memorandum 09-012, other sources as determined by the Department of Defense Component or local commander. The Navy’s Commercial Credential Source also conducts initial commercial background checks prior to creation of credential, and prior to forwarding to the installation for credential inspection and final government screening using Department of Defense authorized authoritative sites and identity verification. Additionally, the Navy’s Commercial Credential Source also provides a 92-day commercial update check and a more comprehensive commercial check annually (aligned with reenrollment). The current Commercial Credential Source (EiD Passport) is certified to issue Personal Identity Verification-Interoperable credentials that meet all Federal Information Processing Standards 201 requirements. These upgraded and federally sanctioned non-Federally Issued credentials are being phased in across the Commander, Navy Installation Command enterprise in the continental United States, Hawaii and Guam and are expected to be complete by end of 2014.

Issuance of Department of Defense authorized TESLIN Identification cards for military retirees, active duty dependents, retired Department of Defense civilians and other eligible populations. Department of Defense also issues seven credentials in different colors and on different DD Form stock. Commonly thought of as Dependent identification or Military Retiree identification cards, there are actually seven variants for different eligible categories. TESLIN cards are easily reproducible, are low tech, and are a non-Federal Information Processing Standards 201 credential. Dependents and retirees, as well as many other categories do not receive any background vetting. There exists no expiration on older retiree identification cards.

Navy procedures regarding the eligibility for security clearances closely adhere and are aligned with procedures set forth in Department of Defense Instruction 5200.2-R. The Department of the Navy funds Personnel Security Investigations through a centrally managed account within Budget Submitting Organization 12. This includes investigation to determine eligibility for federal employment and initial National Security Investigations, and periodic reinvestigations to determine eligibility for access to classified information. Although centrally funded, the initiation of Personnel Security Investigations requests is decentralized and relies on unit security managers to verify and validate the need for Personnel Security Investigations prior to submission. Once submitted by the command, the Department of the Navy is obligated to pay for the investigation. Currently, there is no automated link between the Joint Personnel Adjudication System and the personnel databases to assist the command security manager in determining whether a Personnel Security Investigation is actually required. Without an authoritative source for determining Personnel Security Investigation requirements, the process is subject to fraud, waste and abuse.

Recommendation 14.1.1. Expedite funding for the existing Department of Defense plan to upgrade TESLIN cards to a more secure media. The card substrate will include multiple overt and covert security features that will address current card security vulnerabilities.

Recommendation 14.1.2. Improve personnel security investigation resourcing by including it in the “Total Ownership Cost” of Department of the Navy manpower.

Recommendation 14.1.3. Establish a link between manpower databases and the Joint Personnel Adjudication System to provide security managers with an authoritative source for making Personnel Security Investigation submission decisions.

Recommendation 14.1.4. Review civilian position descriptions and military billets to ensure security clearance requirements are clearly identified to facilitate Department of the Navy level planning, programming and budgeting activities.

Recommendation 14.1.6. Implement an automated Continuous Evaluation Program to identify potentially derogatory information that may affect an individual’s security clearance eligibility and/or a Department of the Navy issued credential.

Recommendation 14.1.7. Update personnel security policy to clearly state requirements for self-reporting of potentially derogatory information.

Recommendation 14.1.8. Reinforce--through training--the requirement for individuals, peers, supervisors and commanders to report potentially disqualifying information through the Joint Personnel Adjudication System to the Department of Defense Consolidated Adjudication Facility.

Finding 14.2. (Major) Although the Navy's vetting and credentialing procedures used for base access and security clearances by the Department of the Navy are in accordance with Department of Defense policy and directives, those processes may not adequately mitigate the potential for insider attack. *(U.S. Fleet Forces Force Protection Baseline Review and Deputy Under-Secretary of the Navy for Plans, Policy, Operations, and Integration input)*

Discussion. The Navy's defense-in-depth model is designed to thwart external threats. Inherent to this model is the assumption that those that have been authorized access to Navy installations do not pose a threat to the assets and personnel located on those installations.

The process of vetting and credentialing for populations that require access to Navy installations differs significantly according to their respective access purposes. These populations include Active Duty and Reserve personnel, government employees, contractors, family members, retirees (military and government service) and vendors. While some populations routinely undergo background investigations and periodic reinvestigation in order to maintain their credentials, others are vetted only once, and then continue to retain their access and credentials until revoked or surrendered.

A significant segment of the above populations that are authorized access to Navy installations are issued TESLIN card credentials. Although TESLIN card credentials may appear similar to Common Access Card credentials, they do not possess all of the (smart card) tamper resistant features, nor are they loaded with a certificate on a chip that enables authentication at a high level of trust. Additionally, future physical access control systems designed to leverage smart card capabilities may not function with TESLIN card credentials.

Current security clearance eligibility periodic review processes allow for significant periods of time between reviews. Accordingly, individuals who have left military service may still be authorized to have their security clearance eligibility re-instated without further review as long as they are still within the required window of periodicity for that clearance level. Additionally, these individuals may not have been under the Continuous Evaluation Program during this time period, leading to situations where aberrant behavior that should have been captured under the Continuous Evaluation Program goes unreported.

The current Continuous Evaluation Program is not completely effective because real world experience has shown that the threshold at which an individual exhibits behavior aberrant enough to warrant intervention by his coworkers or supervisors is above the level of behavior that may actually be indicative of real risk.

Recommendation 14.2.1. Review periodicity requirements and methodology for security clearance eligibility of active duty military personnel, government service civilians and contractors.

Recommendation 14.2.2. Determine whether periodic background vetting is warranted for military family members, military retirees and civil service retirees to enable continued installation access.

Recommendation 14.2.3. Determine the necessity for migration to Common Access Cards for current TESLIN populations to enable authentication at a high level of trust and deployment of future physical access control systems.

Recommendation 14.2.4. Review the Continuous Evaluation Program to determine if current evaluation criteria and processes can be improved to better mitigate the insider threat.

Task 15. Coordinate with the Assistant Secretary of the Navy (Manpower & Reserve Affairs) and the General Counsel of the Navy, as necessary, regarding the security clearance rapid reviews.

Finding 15.1. The findings and recommendations outlined in the Assistant Secretary of the Navy (Manpower and Reserve Affairs) security clearance rapid reviews are aligned and complimentary to the findings and recommendations regarding vetting, credentialing and security clearances contained in this report. *(Secretary of the Navy Action Memorandum of October 10, 2013)*

Discussion. A thorough review of the security clearance rapid reviews and coordination with the Office of the Assistant Secretary of the Navy (Manpower and Reserve Affairs) and General Counsel of the Navy determined that, although the recommended actions resulting from the rapid reviews are generally directed at a higher level than those contained in this report, they remain aligned in their respective intent and are complementary to the actions being taken throughout the spectrum of authorities.

Recommendation 15.1. Implement the recommendations outlined in the Assistant Secretary of the Navy (Manpower and Reserve Affairs) security clearance rapid reviews.

5. Physical Security and Access Control Policy and Guidance Directives

a. Presidential and Department of Defense policy and guidance directives

- Presidential memorandum: "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs"
- Homeland Security Presidential Directive 12, "Policies for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
- Secretary of Defense Directive-Type Memorandum 09-012, "Interim Policy Guidance for Department of Defense Physical Access Control," December 8, 2009
- Deputy Secretary of Defense Memorandum, "Antiterrorism Building Standards for Leased Space," December 7, 2012
- Department of Defense Instruction 2000.12, "Department of Defense Antiterrorism Program," September 9, 2013
- Department of Defense Instruction 2000.16, "Department of Defense Antiterrorism Standards," December 8, 2006
- Department of Defense Instruction 5200.08-R, "Physical Security Program," April 9, 2007
- Department of Defense Instruction 5200.08, "Security of Department of Defense Installations and Resources and the Department of Defense Physical Security Review Board," December 10, 2005
- Department of Defense Directive 3000.3, "Policy for Non-Lethal Weapons," July 9, 1996
- Unified Facilities Criteria 4-010-01, "Department of Defense Minimum Antiterrorism Standards for Buildings," February 9, 2012
- FIPS 201, "Federal Information Processing Standards Publication Personal Identity Verification of Federal Employees and Contractors," June 23, 2006
- 10 U.S.C. Subtitle C, Authority, Law Enforcement, Security of Naval Installations, Security of Department of Defense Installations

b. U.S. Navy policy and guidance directives

- SECNAV M-5510.30, "DoN Personnel Security Program," June 2006
- SECNAV M-5510.36, "DoN Information Security Program," June 2006
- SECNAVINST 5510.37 "DoN Insider Threat Program," August 8, 2013
- SECNAV Directed Installation Security Posture Assessment, September 17, 2013
- CNO Antiterrorism Strategic Guidance 2010, September 2010

- OPNAVINST 3400.12, “Navy Required Operational Capability Levels for Navy Installations and Activities,” October 6, 2008
- OPNAVINST 3300.53C, “Navy Antiterrorism Program,” May 26, 2009
- OPNAVINST 5530.14E, “Navy Physical Security and Law Enforcement Program,” January 28, 2009
- OPNAVINST 3591.1F, “Small Arms Training and Qualification,” August 12, 2009
- Navy-wide OPTASK Antiterrorism, March 18, 2013
- U.S. Fleet Forces, Antiterrorism Operations Order 3300-13, January 2013
- U.S. Pacific Fleet, Operations Order 201, September 2007
- U.S. Naval Forces Southern Command, Operations Order 4000-07, October 2007
- U.S. Naval Forces Europe, Operations Order 4000-05 April 2006
- U.S. Naval Forces Central Command, Operations Order 09-1, December 2009

c. Geographic Combatant Commander policy and guidance directives

- USNORTHCOM Antiterrorism Instruction 10-222
- USEUCOM Antiterrorism Operations Order 11-05
- USCENTCOM Antiterrorism Operations Order 05-02
- USPACOM Antiterrorism/CIP Operations Order 5050-08
- USSOUTHCOM SC Regulation 380.16
- USAFRICOM AT-CIP Operations Order 10-06

6. Terms of Reference

a. Access Control. An integral and interoperable part of Department of Defense installation physical security programs. Each installation commander and facility director must clearly define, consistent with Department of Defense policy, the access control measures (tailored to local conditions) required to safeguard personnel, facilities, protect capabilities and accomplish the mission.
b. Force Protection. Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities and critical information. Force protection does not include actions to defeat the enemy or protect against accidents, weather or disease.
c. Insider Threat. A person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism or kinetic actions resulting in loss or degradation of resources or capabilities. The term kinetic can include, but is not limited to, the threat of harm from sabotage or workplace violence.
d. Physical Security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material and documents; and to safeguard them against espionage, sabotage, damage and theft.
e. Risk. Probability and severity of loss linked to hazards.
f. Tactical Control. Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed and, usually, local direction and control of movements or maneuvers necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to and exercised at any level at or below the level of combatant command.
g. Tactical Control for Force Protection. Tactical Control that enables the Geographic Combatant Commander to order implementation of force protection measures and to exercise the security responsibilities outlined in any Memorandum of Agreement concluded pursuant to Memorandum of Understanding between the Department of State and the Department of Defense, “Security of Department of Defense Elements and Personnel in Foreign Areas,” December 16, 1997 (known as the “Universal MOU”). Further, Tactical Control for Force Protection authorizes the Geographic Combatant Commander to change, modify, prescribe and enforce force protection measures for covered forces. This relationship includes the authority to inspect and assess security requirements, and submit budget requests to parent organizations to fund identified corrections. The Geographic Combatant Commander may also direct immediate Force Protection Condition measures (including temporary relocation and departure) when in his judgment such measures must be accomplished

without delay to ensure the safety of Department of Defense personnel involved. Persons subject to Tactical Control for Force Protection of a Geographic Combatant Commander include Active and Reserve Component personnel (including National Guard personnel in a title 10 status) in the Area of Responsibility.